IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

First Named Inventor :	Louis Guillou et al.	
Appln. No :	09/889.918	
Filed :	January 27, 2000	Group Art Unit: 2131
For :	METHOD FOR PROVING THE AUTHENTICITY OR INTEGRITY OF A MESSAGE BY MEANS OF A PUBLIC EXPONENT EQUAL TO THE POWER OF TWO	Examiner: Matthew T. Henning
Patent No.:	7,386,122	
Issued :	June 10, 2008	
Docket No.:	F40.12-0050	

REQUEST FOR CERTIFICATE OF CORRECTION

ELECTRONICALLY FILED AUGUST 20, 2008

Sir:

In conformity with 37 C.F.R. § 1.322, applicant hereby requests a Certificate of Correction in connection with the above-identified patent.

Form PTO-1050 entitled CERTIFICATE OF CORRECTION setting out the printer's errors has been completed and is enclosed. It is respectfully requested that the enclosed Certificate be approved and signed by an Attesting Officer, and that a copy be returned to applicant's attorney for attachment to the original Certificate of Letters Patent.

Errors requested to be corrected are USPTO printing errors, so no fee is required.

The Director is authorized to charge any fee deficiency required by this paper or credit any overpayment to Deposit Account No. 23-1123. A duplicate of this communication is enclosed.

Respectfully submitted,

WESTMAN, CHAMPLIN & KELLY, P.A.

By:_____/David D. Brush_____
   David D. Brush, Reg. No. 34,557
   Suite 1400 - International Centre
   900 Second Avenue South
   Minneapolis, Minnesota 55402-3319
   Phone: (612) 334-3222 Fax: (612) 334-3312

DDB:akb

(Also Form PTO-1050)

UNITED STATES PATENT AND TRADEMARK OFFICE
CERTIFICATE OF CORRECTION

PATENT NO : 7,386,122 B1

DATED : June 10, 2008

INVENTOR(S) : Louis Guillou et al.

It is certified that error appears in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

Column 7
Line 54 delete "$r_i \ Q_{i,1}{}^{d1}$" and insert -- $r_i \cdot Q_{i,1}{}^{d1}$ --.

Column 16
Line 46 delete "$D^v G_1{}^{d1}$" and insert -- $D^v / G_1{}^{d1}$ --.

Column 24
Line 1 delete "mode" and insert -- mod --.
Line 10 delete "mode" and insert -- mod --.
Line 11 delete "mode" and insert -- mod --.

Column 27
Line 15 delete "$d - d_1$" and insert -- $d = d_1$ --.

Column 28
Line 58 delete "$G_i^{d'} i$" and insert -- G_i^{di} --.

Column 30
Line 43 delete "$G_1^{68_1 d_1}$" and insert -- $G_1^{\varepsilon_1 d_1}$ --.

Column 31
Line 10 delete "$Q_{1hu\ d}{}^{1}$" and insert -- $Q_1^{d_1}$ --.

Line 11 delete "Qm^{d_m}" and insert -- $Q_m^{d_m}$ --.

Line 40 delete "Mis" and insert -- M is --.

Line 53 delete "F,: and insert -- f , --.

Line 56 delete "$G_1^{\varepsilon_1 d_2}$" and insert -- $G_1^{\varepsilon_1 d_1} \cdot G_2^{\varepsilon_2 d_2}$ --.

Line 61 delete "$0 \leqq d_i \leqq 2^k$" and insert -- $0 \leq d_i \leq 2^k$ --.

Line 64 delete "on eor" and insert -- one or --.

<u>Column 32</u>

Line 17 delete "R^i" and insert -- R_i --.

Line 36 delete "Dm^v" and insert -- D_m^v --.

<u>Column 33</u>

Line 3 delete "$Gm^{\varepsilon_m d_m}$" and insert -- $G_m^{\varepsilon_m d_m}$ --.

Line 44 delete "$Gm^{\varepsilon_m d_m}$" and insert -- $G_m^{\varepsilon_m d_m}$ --.

<u>Column 34</u>

Line 14 delete "$Gm^{\varepsilon_m d_m}$" and insert -- $G_m^{\varepsilon_m d_m}$ --.

Line 20 after "method", insert a hard return.

Line 42 delete "F," and insert -- f, --.

Line 51 delete "F," and insert -- f, --.

Line 55 delete "$Gm^{\varepsilon_m d_m}$" and insert -- $G_m^{\varepsilon_m d_m}$ --.

<u>Column 35</u>

Line 9 delete "eachof" and insert -- each of --.

Line 17 delete "R^i" and insert -- R_i --.

<u>Column 36</u>

Line 14 delete "$G_f^{\varepsilon_1 d_1}$" and insert -- $G_1^{\varepsilon_1 d_1}$ --.

Line 15 delete "$G_2^{\varepsilon_2 d_d}$" and insert -- $G_2^{\varepsilon_2 d_2}$ --.